

1 ROBBINS GELLER RUDMAN
& DOWD LLP
2 SHAWN A. WILLIAMS (213113)
Post Montgomery Center
3 One Montgomery Street, Suite 1800
San Francisco, CA 94104
4 Telephone: 415/288-4545
415/288-4534 (fax)
5 shawnw@rgrdlaw.com

6 ROBBINS GELLER RUDMAN
& DOWD LLP
7 PAUL J. GELLER
120 East Palmetto Park Road, Suite 500
8 Boca Raton, FL 33432
Telephone: 561/750-3000
9 561/750-3364 (fax)
pgeller@rgrdlaw.com

10 LABATON SUCHAROW LLP
11 JOEL H. BERNSTEIN
140 Broadway, 34th Floor
12 New York, NY 10005
Telephone: 212/907-0700
13 212/818-0477 (fax)
jbernstein@labaton.com

EDELSON PC
JAY EDELSON
350 North LaSalle Street, 13th Floor
Chicago, IL 60654
Telephone: 312/589-6370
312/589-6378 (fax)
jedelson@edelson.com

14 Interim Co-Lead Counsel for Plaintiffs

15 [Additional counsel appear on signature page.]

16 UNITED STATES DISTRICT COURT
17 NORTHERN DISTRICT OF CALIFORNIA
18 SAN FRANCISCO DIVISION

19 CARLO LICATA, ADAM PEZEN and)
20 NIMESH PATEL, Individually and on Behalf)
of All Others Similarly Situated,)
21 Plaintiffs,)

22 vs.)

23 FACEBOOK, INC.,)
24)

25 Defendant.)

Case No. 3:15-cv-03747-JD

CONSOLIDATED CLASS ACTION
COMPLAINT

*Consolidated with: Nos. 3:15-cv-03748 and
3:15-cv-03749*

DEMAND FOR JURY TRIAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Adam Pezen, Carlo Licata, and Nimesh Patel bring this Consolidated Class Action Complaint (“Complaint”) against Defendant Facebook, Inc. (“Facebook”) to put a stop to its surreptitious collection, use, and storage of Plaintiffs’ and the proposed Class’s sensitive biometric data. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

NATURE OF THE ACTION

1. Defendant Facebook operates the largest social network in the world, with over one billion active users.

2. Facebook users can use its platform to, among other things, upload and share photographs with friends and relatives. Once a user uploads a photograph on Facebook, the user can “tag” (*i.e.*, identify by name) other Facebook users and non-users who appear in the photograph.

3. To encourage use of the tagging feature, Facebook launched a program in 2010 called “Tag Suggestions.” Tag Suggestions functions by scanning photographs uploaded by the user and then identifying faces appearing in those photographs. If Tag Suggestions recognizes and identifies one of the faces appearing in the photograph, Facebook will suggest that individual’s name or automatically tag them.

4. Facebook conceals that Tag Suggestions uses proprietary facial recognition software to extract from user-uploaded photographs the unique biometric identifiers (*i.e.*, graphical representations of facial features, also known as facial geometry) associated with people’s faces and identify who they are. Facebook does not disclose its biometrics data collection to its users, nor does it even ask users to acknowledge, let alone consent to, these practices.

5. Through these practices, Facebook not only disregards its users’ privacy rights; it also violates the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the “BIPA”), which was specifically designed to protect Illinois residents from practices like Facebook’s. In particular, Facebook violated (and continues to violate) the BIPA because it did not:

- 1 • Properly inform Plaintiffs or the Class in writing that their biometric
2 identifiers (face geometry) were being generated, collected or stored;
- 3 • Properly inform Plaintiffs or the Class in writing of the specific purpose and
4 length of time for which their biometric identifiers were being collected,
5 stored, and used;
- 6 • Provide a publicly available retention schedule and guidelines for
7 permanently destroying the biometric identifiers of Plaintiffs and the Class
8 (who do not opt-out of “Tag Suggestions”); and
- 9 • Receive a written release from Plaintiffs or the Class to collect, capture, or
10 otherwise obtain their biometric identifiers.

11 6. Accordingly, this Complaint seeks an order: (i) declaring that Facebook’s conduct
12 violates the BIPA; (ii) requiring Facebook to cease the unlawful activities discussed herein; and
13 (iii) awarding statutory damages to Plaintiffs and the proposed Class.

14 **PARTIES**

15 7. Plaintiff Adam Pezen (“Pezen”) is a natural person and Facebook user. Plaintiff is a
16 resident and citizen of the State of Illinois.

17 8. Plaintiff Carlo Licata (“Licata”) is a natural person and Facebook user. Plaintiff is a
18 resident and citizen of the State of Illinois.

19 9. Plaintiff Nimesh Patel (“Patel”) is a natural person and Facebook user. Plaintiff is a
20 resident and citizen of the State of Illinois.

21 10. Defendant Facebook, Inc. is a Delaware corporation with its principal executive
22 offices and corporate headquarters located at 1601 Willow Road, Menlo Park, California 94025.
23 Facebook is a citizen of the States of Delaware and California. Facebook is also registered to
24 conduct business in the State of Illinois (file number 66267067) and maintains an office in Cook
25 County, Illinois. Facebook conducts business throughout this District, the State of Illinois, the State
26 of California, and the United States.

27 **JURISDICTION AND VENUE**

28 11. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28
U.S.C. §1332(d) (“CAFA”), because: (i) the proposed Class consists of well over 100 members;
(ii) the parties are minimally diverse, as members of the proposed Class, including Plaintiffs, are

1 citizens of a state different from Defendant’s home state; and (iii) the aggregate amount in
2 controversy exceeds \$5,000,000, exclusive of interests and costs.

3 12. This Court has personal jurisdiction over Plaintiffs because Plaintiffs submit to the
4 Court’s jurisdiction. This Court has personal jurisdiction over Defendant Facebook because
5 Defendant has submitted to this Court’s jurisdiction and has its corporate headquarters in Menlo
6 Park, California.

7 13. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant
8 maintains its corporate headquarters and principal place of business in this District.

9 **INTRADISTRICT ASSIGNMENT**

10 14. Pursuant to Civil Local Rule 3-2(d), this case should be assigned to the San Francisco
11 Division.

12 **FACTUAL BACKGROUND**

13 **I. Biometrics and Consumer Privacy**

14 15. “Biometrics” refers to technologies used to identify an individual based on unique
15 physical characteristics. Common biometric identifiers include retina or iris scans, fingerprints, or
16 hand or face geometry scans, which are all generally obtained by first acquiring an image or
17 photograph of the biometric identifier. One of the most prevalent uses of biometrics is facial
18 recognition technology, which works by scanning an image for human faces, extracting facial feature
19 data from a photograph or image of a human face, generating a “faceprint” from the image through
20 the use of facial-recognition algorithms, and then comparing, or “matching,” the resultant faceprint
21 to other faceprints stored in a “faceprint database.” If a database match is found, a person may be
22 identified.

23 16. The recent sophistication of facial recognition software has generated many
24 commercial applications of the technology, but also raised serious privacy concerns about its
25 massive scale, scope, and surreptitiousness.¹ During a 2012 U.S. Senate hearing, Senator Al Franken

26 _____
27 ¹ *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the*
28 *Subcomm. on Privacy Tech & the Law of the S. Comm. on the Judiciary, 112th Cong. 1 (2012)*
(statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), *available at*
https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf.

1 noted that someone armed with a faceprint can find that person’s “name . . . social networking
 2 account and . . . can find and track [them] in the street, in the stores [they] visit, the government
 3 buildings [they] enter, and the photos [their] friends post online.”² Faceprints can even be used to
 4 identify protesters from afar and then “target them for selective jailing and prosecution.”³

5 17. Unlike other identifiers such as Social Security or credit card numbers, which can be
 6 changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot.
 7 These unique and permanent biometric identifiers, once exposed, leave victims with no means to
 8 prevent identity theft and unauthorized tracking. Recognizing this, the Federal Trade Commission
 9 urged companies using facial recognition technology to ask for consent *before* ever scanning and
 10 extracting biometric data from their digital photographs.⁴ Facebook has deliberately ignored this
 11 prevailing view, which is expressly required under the BIPA, failed to obtain user consent before
 12 launching its wide-spread facial recognition program, and continues to violate millions of Illinois
 13 residents’ legal privacy rights.

14 **II. Illinois’s Biometric Information Privacy Act**

15 18. The BIPA was enacted in 2008. Under the BIPA, companies may not “collect,
 16 capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric
 17 identifier . . . unless it first:

18 (1) informs the subject . . . in writing that a biometric identifier . . . is being collected
 19 or stored;

20 (2) informs the subject . . . in writing of the specific purpose and length of term for
 21 which a biometric identifier . . . is being collected, stored, and used; and

22 (3) receives a written release executed by the subject of the biometric identifier”

23 740 ILCS 14/15(b).

24 ² *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the*
 25 *Subcomm. on Privacy Tech & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012)
 (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm.
 on the Judiciary), *available at* http://www.franken.senate.gov/?p=press_release&id=2144.

26 ³ *Id.*

27 ⁴ *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*,
 28 Federal Trade Commission (Oct. 2012), *available at* <http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf>.

1 19. The statute defines “biometric identifier” to include “a retina or iris scan, fingerprint,
2 voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.

3 20. The BIPA also regulates how companies must handle Illinois residents’ biometric
4 data. *See, e.g.*, 740 ILCS 14/15(c)–(d). For instance, the BIPA prohibits selling, leasing, trading, or
5 otherwise profiting from a person’s biometric data, 740 ILCS 14/15(c), and requires that companies
6 develop a publicly available written policy establishing a retention schedule and guidelines for
7 permanently destroying biometric data when the initial purpose for collecting such data has been
8 satisfied or within three years of the individual’s last interaction with the company, whichever occurs
9 first. 740 ILCS 14/15(a).

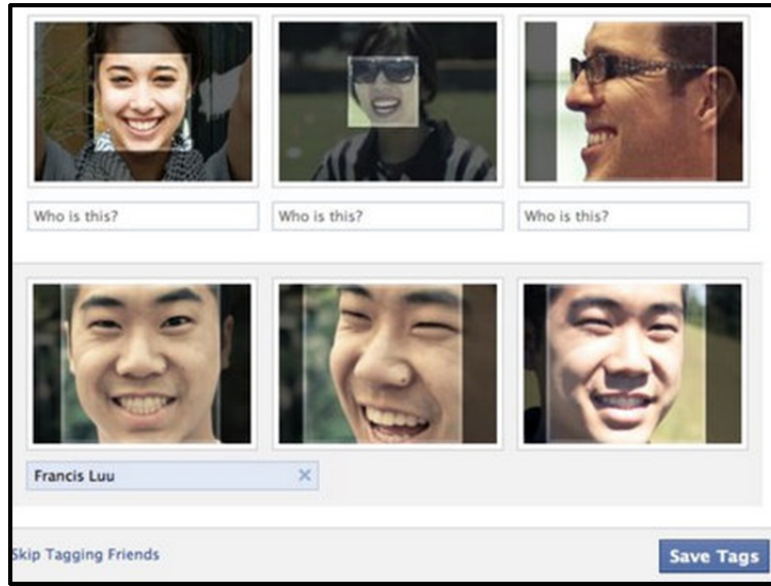
10 **III. Facebook Violates the Biometric Information Privacy Act**

11 21. In 2010, Facebook launched a program called “Tag Suggestions,” which claimed to
12 “automate the process of identifying and, if the user chooses, tagging friends in the photos he or she
13 uploads.”⁵

14 22. Unbeknownst to the public, Tag Suggestions relies on state-of-the-art facial
15 recognition technology to extract biometric identifiers from user-uploaded photographs in order to
16 determine who the people in the photographs are. Figure 1 below shows an example of what Tag
17 Suggestions looks like to a Facebook user.

18
19
20
21
22
23
24
25
26
27 ⁵ *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the*
28 *Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012)
(statement of Robert Sherman, Manager of Privacy and Public Policy, Facebook, Inc.), available at
<http://www.judiciary.senate.gov/imo/media/doc/12-7-18ShermanTestimony.pdf>.

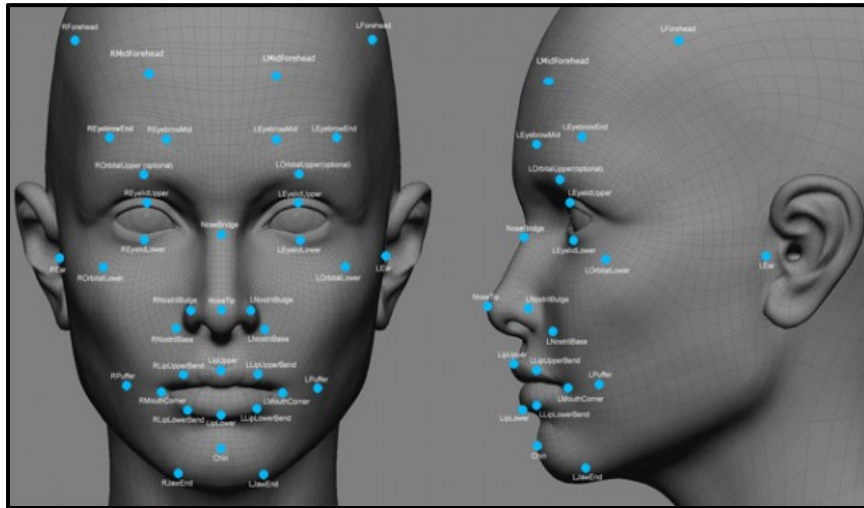
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



(Fig. 1.)

23. Facebook uses facial recognition software to extract biometric data from user-uploaded photographs through the use of an algorithm that calculates a unique digital representation of the face (which it calls a “template”) based on geometric relationship of their facial features, like the distance between their eyes, nose and ears.

24. “Template” data (or, alternatively, faceprint data) stored by Facebook is a form of a biometric identifier extracted from the image of a person’s face (*i.e.*, including information about the geometry of their face). (See Figure 2, showing an example of geometric data points of a human face.)



(Fig. 2.)

25. The process for creating image-based biometric identifiers (including those Facebook collects) is largely the same. In each case, an algorithm is used to calculate an individual's unique physical characteristics, which results in a biometric template that is separate and distinct from the image from which it was created.

26. Without even informing its users – let alone obtaining their informed written consent – Facebook through Tag Suggestions automatically enrolled them into its facial recognition program and extracted biometric identifiers from their uploaded photographs and previously tagged pictures, and stored these biometric identifiers in a database.

27. Because Facebook users were only allowed to opt out of the program *after the fact* (and even then, only if they knew to look for the opt-out mechanism), Facebook users unwittingly had their biometric identifiers extracted from photographs and then stored – a practice that continues to this day.

A. Facebook Never Requires Users to Acknowledge Its Biometric Data Collection Practices, Never Obtains Their Express Written Consent to Collect the Same, and, Instead, Hides the Fact that It Systematically Collects Users' Biometrics

28. Since Tag Suggestions debuted in 2010, Facebook has been intentionally elusive in explaining how the technology works. First, Facebook does not directly inform users that it collects, captures, and obtains faceprints from users. In fact, even though Tag Suggestions has been in use for five years, Facebook still does not require users to acknowledge its collection of their biometric data,

1 much less obtain a written release from them before collecting their faceprints. Instead, Facebook
2 markets Tag Suggestions as a convenience feature, often with advertisements under the heading
3 “Photos are better with friends.” And nothing in those seemingly innocuous advertisements gives
4 any indication that use of the feature would come at the cost of users’ biometric privacy rights.⁶

5 29. Second, Facebook’s Tag Suggestions are an opt-out (not an opt-in) program, so by
6 default all users are automatically signed up. Facebook makes it difficult to opt out: In fact, since the
7 Tag Suggestions feature was rolled out, Facebook has kept its biometrics data collection practices
8 out of its privacy policies and has instead placed ambiguous statements about the true nature of its
9 Tag Suggestions program on remote sections of its website (such as in its “Help Center” or the now
10 defunct “Notes” sections). Uncovering these remote sections not only requires a user to know about
11 Tag Suggestions in the first place, but also requires them to affirmatively seek out more information
12 through multiple layers of additional pages.

13 30. Third, and compounding that problem and its violation of the BIPA, Facebook’s
14 website does not have a written, publicly available policy identifying its biometrics retention
15 schedule, nor guidelines for permanently destroying users’ (who do not opt-out of “Tag
16 Suggestions”) biometric identifiers when they are no longer needed.

17 31. By and through these actions, Facebook not only disregarded Plaintiffs and the
18 Class’s privacy rights, but it also violated their statutorily protected rights under BIPA to control the
19 collection, use, and storage of their sensitive biometric data. Ignoring backlash over its unlawful
20 biometric data collection practices, Facebook continues to roll out new products using facial
21 recognition technology. Specifically, in June 2015, Facebook introduced a new mobile application,
22 called Moments, that purports to allow Facebook users to more easily share photographs taken on
23 users’ mobile devices. This application also uses Facebook’s proprietary facial recognition
24 technology to extract biometric identifiers (including their face geometry) from photographs taken

25 _____
26 ⁶ Facebook has not disclosed whether it will sell or lease its enormous database of faceprints to
27 other companies for their facial recognition programs. *See, e.g., Facebook Hit With Tough Questions*
28 *On Facial Recognition In Senate Hearing*, VentureBeat, available at
<http://venturebeat.com/2012/07/18/facebook-hit-with-tough-questions-on-facial-recognition-in-senate-hearing/> (last visited Aug. 24, 2015).

1 on a users' mobile device and identify others in those pictures. Facebook does not offer Moments in
2 the Europe Union because of regulators' concerns about its facial recognition technology.

3 **IV. Plaintiffs' Experiences**

4 **A. Plaintiff Adam Pezen's Experience**

5 32. Plaintiff Adam Pezen has been a Facebook user since 2005. Since then, Pezen has
6 uploaded photographs to his account that include images of his face and has been tagged in many of
7 them. Pezen has also been tagged in photographs uploaded by other Facebook members without his
8 knowledge or consent.

9 33. Pezen never consented, agreed, or gave permission – written or otherwise – to
10 Facebook to collect or store his biometric identifiers. Further, Pezen was never provided with nor
11 ever signed a written release allowing Facebook to collect or store his biometric identifiers.

12 34. Facebook never informed Pezen by written notice or otherwise that he could prevent
13 Facebook from collecting, storing or using his biometric identifiers.

14 35. Likewise, Pezen was never provided with an opportunity to prohibit or prevent
15 Facebook from collecting, storing or using his biometric identifiers.

16 36. Nevertheless, when Pezen uploaded photographs to his account and made them his
17 profile pictures, and also when he was tagged in photographs by other Facebook members without
18 his knowledge or consent, Facebook extracted from those photographs a unique faceprint or
19 “template” for him containing his biometric identifiers, including his facial geometry, and identified
20 who he was. Facebook subsequently stored Pezen's biometric identifiers in its databases.

21 37. As a result of Facebook's unauthorized collection and use of Pezen's biometric
22 identifiers, Pezen was deprived of his control over that valuable information. By depriving him of
23 his control over this valuable information, Facebook misappropriated the value of his biometric
24 identifiers.

25 38. Pezen has additionally suffered damages in the diminution in value of his sensitive
26 biometric identifiers.

27
28

1 **B. Plaintiff Carlo Licata’s Experience**

2 39. Plaintiff Carlo Licata has been a Facebook user since 2009. Since then, Licata has
3 uploaded photographs to his account – including those used for his profile pictures – and has been
4 tagged in photographs by friends.

5 40. Licata never consented, agreed, or gave permission – written or otherwise – to
6 Facebook to collect or store his biometric identifiers. Further, Licata was never provided with nor
7 ever signed a written release allowing Facebook to collect or store his biometric identifiers.

8 41. Facebook never informed Licata by written notice or otherwise that he could prevent
9 Facebook from collecting, storing or using his biometric identifiers.

10 42. Likewise, Licata was never provided with an opportunity to prohibit or prevent
11 Facebook from collecting, storing or using his biometric identifiers.

12 43. Nevertheless, when Licata uploaded photographs to his account and made them his
13 profile pictures and also when he was tagged in photographs, Facebook extracted from those
14 photographs a unique faceprint or “template” for him containing his biometric identifiers, including
15 his facial geometry, and identified who he was. Facebook subsequently stored Licata’s biometric
16 identifiers in its databases.

17 44. As a result of Facebook’s unauthorized collection and use of Licata’s biometric
18 identifiers, Licata was deprived of his control over that valuable information. By depriving him of
19 his control over this valuable information, Facebook misappropriated the value of his biometric
20 identifiers.

21 45. Licata has additionally suffered damages in the diminution in value of his sensitive
22 biometric identifiers.

23 **C. Plaintiff Nimesh Patel’s Experience**

24 46. Plaintiff Nimesh Patel has been a Facebook user since at least 2008. Since then, Patel
25 has uploaded photographs to his account and has been tagged in photographs by friends.

26 47. Patel never consented, agreed, or gave permission – written or otherwise – to
27 Facebook to collect or store his biometric identifiers. Further, Patel was never provided with nor ever
28 signed a written release allowing Facebook to collect or store his biometric identifiers.

1 48. Facebook never informed Patel by written notice or otherwise that he could prevent
2 Facebook from collecting, storing or using his biometric identifiers.

3 49. Likewise, Patel was never provided with an opportunity to prohibit or prevent
4 Facebook from collecting, storing or using his biometric identifiers.

5 50. Nevertheless, when Patel uploaded photographs to his account and when he was
6 tagged in photographs, Facebook extracted from those photographs a unique faceprint or “template”
7 for him containing his biometric identifiers, including his facial geometry, and identified who he
8 was. Facebook subsequently stored Patel’s biometric identifiers in its databases.

9 51. As a result of Facebook’s unauthorized collection and use of Patel’s biometric
10 identifiers, Patel was deprived of his control over that valuable information. By depriving him of his
11 control over this valuable information, Facebook misappropriated the value of his biometric
12 identifiers.

13 52. Patel has additionally suffered damages in the diminution in value of his sensitive
14 biometric identifiers.

15 **CLASS ALLEGATIONS**

16 53. **Class Definition:** Plaintiffs Pezen, Licata, and Patel bring this action pursuant to Rule
17 23 of the Federal Rules of Civil Procedure on behalf of themselves and a class of similarly situated
18 individuals, defined as follows:

19 All persons who had their biometric identifiers, faceprints, or face templates
20 collected, captured, received, or otherwise obtained by Facebook while residing in
Illinois.

21 The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this
22 action and members of their families; (2) Defendant, Defendant’s subsidiaries, parents, successors,
23 predecessors, and any entity in which the Defendant or its parents have a controlling interest and its
24 current or former employees, officers and directors; (3) persons who properly execute and file a
25 timely request for exclusion from the Class; (4) persons whose claims in this matter have been
26 finally adjudicated on the merits or otherwise released; (5) Plaintiffs’ counsel and Defendant’s
27 counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

28

1 54. **Numerosity:** The exact number of Class members is unknown to Plaintiffs at this
2 time, but it is clear that individual joinder is impracticable. Defendant has collected, captured,
3 received, or otherwise obtained biometric identifiers from at least thousands (and potentially even
4 millions) of individuals who fall into the definition of the Class. Ultimately, the Class members will
5 be easily identified through Defendant's records.

6 55. **Commonality and Predominance:** There are many questions of law and fact
7 common to the claims of Plaintiffs and the Class, and those questions predominate over any
8 questions that may affect individual members of the Class. Common questions for the Class include
9 the following:

10 (a) whether Facebook collected, captured, received, or otherwise obtained
11 Plaintiffs' and the Class's biometric identifiers;

12 (b) whether Facebook properly informed Plaintiffs and the Class that it collected,
13 used, and stored their biometric identifiers;

14 (c) whether Facebook obtained a written release (as defined in 740 ILCS 14/10)
15 from Plaintiffs and the Class to collect, capture, or otherwise obtain their biometric identifiers;

16 (d) whether Facebook has sold, leased, traded, or otherwise profited from
17 Plaintiffs' and the Class's biometrics identifiers;

18 (e) whether Facebook had and made available to the public, a written policy
19 establishing a retention schedule and guidelines for permanently destroying biometric identifiers in
20 compliance with the BIPA; and

21 (f) whether Facebook's violations of the BIPA were committed intentionally,
22 recklessly, or negligently.

23 56. **Typicality:** Plaintiffs' claims are typical of the claims of all other members of the
24 Class. Plaintiffs and the Class members sustained substantially similar damages as a result of
25 Defendant's uniform wrongful conduct, based upon the same transactions that were made uniformly
26 with Plaintiffs and the Class.

27 57. **Adequate Representation:** Plaintiffs will fairly and adequately represent and protect
28 the interests of the Class. Plaintiffs have retained counsel with substantial experience in prosecuting

1 written release executed by the subject of the biometric identifier” 740 ILCS 14/15(b)
2 (emphasis added).

3 62. Facebook is a Delaware corporation and thus qualifies as a “private entity” under the
4 BIPA. *See* 740 ILCS 14/10.

5 63. As explained in detail in Section III, above, Plaintiffs’ and the Class’s faceprints or
6 face geometry are “biometric identifiers” pursuant to 740 ILCS 14/10.

7 64. Facebook systematically and automatically collected, used, and stored Plaintiffs’ and
8 the Class’s biometric identifiers without first obtaining the specific written release required by 740
9 ILCS 14/15(b)(3).

10 65. As explained in Section III.A, Facebook did not properly inform Plaintiffs or the
11 Class in writing that their biometric identifiers were being collected and stored, nor did it inform
12 them in writing of the specific purpose and length of term for which their biometric identifiers were
13 being collected, stored, and used as required by 740 ILCS 14/15(b)(1)–(2).

14 66. By collecting, storing, and using Plaintiffs’ and the Class’s biometric identifiers as
15 described herein, Facebook violated Plaintiffs’ and the Class’s rights to privacy in their biometric
16 identifiers as set forth in the BIPA, 740 ILCS 14/1, *et seq.*

17 67. On behalf of themselves and the Class, Plaintiffs seek: (i) injunctive and equitable
18 relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Facebook to
19 comply with the BIPA’s requirements for the collection, storage, and use of biometric identifiers;
20 (ii) statutory damages of \$5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS
21 14/20(2) and statutory damages of \$1,000 per negligent violation of the BIPA pursuant to 740 ILCS
22 14/20(1); and (iii) reasonable attorneys’ fees and costs and other litigation expenses pursuant to 740
23 ILCS 14/20(3).

24 **SECOND CAUSE OF ACTION**

25 **Violation of 740 ILCS 14/15(a)**
26 **(On Behalf of Plaintiffs and the Class)**

27 68. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.
28

1 D. Awarding injunctive and other equitable relief as is necessary to protect the interests
2 of the Class, including, among other things, an order requiring Facebook to collect, store, and use
3 biometric identifiers in compliance with the BIPA;

4 E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys'
5 fees;

6 F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent
7 allowable; and

8 G. Awarding such other and further relief as equity and justice may require.

9 **JURY TRIAL**

10 Plaintiffs demand a trial by jury for all issues so triable.

11 DATED: August 28, 2015

ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS
DAVID W. HALL

14
15 s/ Shawn A. Williams
SHAWN A. WILLIAMS

16 Post Montgomery Center
17 One Montgomery Street, Suite 1800
18 San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)

19 ROBBINS GELLER RUDMAN
20 & DOWD LLP
21 PAUL J. GELLER
22 STUART A. DAVIDSON
23 MARK DEARMAN
24 CHRISTOPHER C. MARTINS
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

25 ROBBINS GELLER RUDMAN
26 & DOWD LLP
27 TRAVIS E. DOWNS III
28 655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

LABATON SUCHAROW LLP
JOEL H. BERNSTEIN
CORBAN S. RHODES
ROSS M. KAMHI
140 Broadway, 34th Floor
New York, NY 10005
Telephone: 212/907-0700
212/818-0477 (fax)

EDELSON PC
JAY EDELSON
ALEXANDER T. H. NGUYEN
350 North LaSalle Street, 13th Floor
Chicago, IL 60654
Telephone: 312/589-6370
312/589-6378 (fax)

Interim Co-Lead Counsel for Plaintiffs

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that on August 28, 2015, I authorized the electronic filing of the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List, and I hereby certify that I caused to be mailed the foregoing document or paper via the United States Postal Service to the non-CM/ECF participants indicated on the attached Manual Notice List.

I certify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on August 28, 2015.

s/ Shawn A. Williams
SHAWN A. WILLIAMS

ROBBINS GELLER RUDMAN
& DOWD LLP
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
E-mail: shawnw@rgrdlaw.com

Mailing Information for a Case 3:15-cv-03747-JD Patel v. Facebook, Inc.

Electronic Mail Notice List

The following are those who are currently on the list to receive e-mail notices for this case.

- **James E Barz**
jbarz@rgrdlaw.com
- **Stuart Andrew Davidson**
sdavidson@rgrdlaw.com,jdennis@rgrdlaw.com,e_file_sd@rgrdlaw.com,e_file_fl@rgrdlaw.com
- **Mark J. Dearman**
mdearman@rgrdlaw.com
- **Paul Jeffrey Geller**
pgeller@rgrdlaw.com
- **Lauren R Goldman**
lrgoldman@mayerbrown.com
- **John Nadolenco**
jnadolenco@mayerbrown.com,los-docket@mayerbrown.com,jaustgen@mayerbrown.com
- **Archis A. Parasharami**
aparasharami@mayerbrown.com
- **Frank Anthony Richter**
frichter@rgrdlaw.com
- **Shawn A. Williams**
shawnw@rgrdlaw.com,ptiffith@rgrdlaw.com,dhall@rgrdlaw.com,e_file_sd@rgrdlaw.com,e_file_sf@rgrdlaw.com

Manual Notice List

The following is the list of attorneys who are **not** on the list to receive e-mail notices for this case (who therefore require manual noticing). You may wish to use your mouse to select and copy this list into your word processing program in order to create notices or labels for these recipients.

Vincent **J. Connelly**
Mayer Brown LLP
71 South Wacker Drive
Chicago, IL 60606

Facebook Inc.
Cooley LLP
3000 El Camino Real
Five Palo Alto Square
Palo Alto, CA 94306-2155